OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

CROSS-SECTOR

22 May 2019 **LIR 190522001**

Federal Hunting License Exception Could Be Exploited by Extremists or Criminal Actors Seeking to Obtain Firearms for Violent Attacks

The FBI's Office of Private Sector (OPS), in collaboration with the FBI Counterterrorism Division (CTD), is providing this LIR to private sector partners to highlight our concern that extremists and other criminal actors could exploit the federal statutory exception that allows non-immigrant visa holders—who are otherwise prohibited from shipping, transporting, receiving, or possessing a firearm or ammunition under 18 U.S.C 922(y)(2)—to legally purchase firearms, including high-capacity military-style rifles, with a valid hunting license or permit. A non-immigrant visa may be issued to a person with permanent residence outside the United States who wishes to be in the United States on a temporary basis. Examples of non-immigrant visas include student, tourist, and business visas. Although at least six states have enacted legislation to restrict non-citizens from purchasing or possessing firearms, [redacted] b7E

[redacted] b7E

[redacted] Although some states, including Hawaii, Illinois, Maine, Massachusetts, New York, and Washington, have enacted legislation prohibiting non-immigrant visa holders from purchasing or possessing firearms, non-immigrant visa holders can legally obtain firearms in most states using the hunting license exception.

The FBI urges state and local authorities, as well as private sector partners, to promptly report suspicious activities related to potential terrorism matters. [redacted] b7E

[redacted] Examples of potential indicators of mobilization to violence can be found in the unclassified booklet, "Homegrown Violent Extremist Mobilization Indicators", which is available at https://go.usa.gov/xEKgd.

Additionally, the FBI's National Tripwire Program provides the below information as potential indicators of criminal activity related to Firearms Shops and Ranges. Each indicator listed may be, by itself, lawful conduct/behavior and may also constitute the exercise of rights guaranteed by the US Constitution. A totality of behavioral indicators and other relevant circumstances should be evaluated when considering law enforcement notification/response.

[redacted] b7E

OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

b7E

If you believe there is an imminent threat, contact your local police as soon as it is safe to do so. You can also report suspicious activity related to the above topic to the FBI's 24-hour tips line by dialing 1-855-TELL-FBI or through the FBI website online at https://tips.fbi.gov.

This LIR was disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices

OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

b7E

If determined that the conduct/behavior is, in fact, suspicious and outside the norm of your work-place environment, law enforcement professionals should be engaged to further examine the circumstances. No single indicator should be the sole basis for law enforcement action. Speech, actions, beliefs, appearances, or Way of Life does not, in and of itself, equate to a suspicious individual.

If safe to do so:

b7E

b7E

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1440633-000

Total Deleted Page(s) = 82
Page 27 ~ Referral/Consult;
Page 28 ~ Referral/Consult;
Page 29 ~ Referral/Consult;
Page 30 ~ Referral/Consult;
Page 31 ~ Referral/Consult;
Page 32 ~ Referral/Consult;
Page 33 ~ Referral/Consult;
Page 34 ~ Referral/Consult;
Page 35 ~ Referral/Consult;
Page 36 ~ Referral/Consult;
Page 37 ~ Referral/Consult;
Page 38 ~ Referral/Consult;
Page 39 ~ Referral/Consult;
Page 40 ~ Referral/Consult;
Page 41 ~ Referral/Consult;
Page 42 ~ Referral/Consult;
Page 43 ~ Referral/Consult;
Page 44 ~ Referral/Consult;
Page 45 ~ Referral/Consult;
Page 46 ~ Referral/Consult;
Page 47 ~ Referral/Consult;
Page 48 ~ Referral/Consult;
Page 49 ~ Referral/Consult;
Page 50 ~ Referral/Consult;
Page 51 ~ Referral/Consult;
Page 52 ~ Referral/Consult;
Page 53 ~ Referral/Consult;
Page 54 ~ Referral/Consult;
Page 76 ~ Referral/Consult;
Page 77 ~ Referral/Consult;
Page 78 ~ Referral/Consult;
Page 79 ~ Referral/Consult;
Page 80 ~ Referral/Consult;
Page 81 ~ Referral/Consult;
Page 82 ~ Referral/Consult;
Page 83 ~ Referral/Consult;
Page 84 ~ Referral/Consult;
Page 85 ~ Referral/Consult;
Page 86 ~ Referral/Consult;
Page 87 ~ Referral/Consult;
Page 88 ~ Referral/Consult;
Page 89 ~ Referral/Consult;
Page 90 ~ Referral/Consult;
Page 91 ~ Referral/Consult;
Page 92 ~ Referral/Consult;
Page 93 ~ Referral/Consult;
Page 158 ~ Duplicate;
Page 159 ~ Duplicate;
Page 160 ~ Duplicate;
Page 161 ~ Referral/Consult;
Page 162 ~ Referral/Consult;
Page 163 ~ Referral/Consult;
Page 164 ~ Referral/Consult;
Page 165 ~ Referral/Consult;
Page 166 ~ Referral/Consult;
Page 167 ~ Referral/Consult;
Page 168 ~ Referral/Consult;
Page 169 ~ Referral/Consult;
Page 170 ~ Referral/Consult;
Page 171 ~ Referral/Consult;
Page 173 ~ Duplicate;
Page 174 ~ Duplicate;
Page 175 ~ Duplicate;
Page 186 ~ Referral/Consult;
Page 187 ~ Referral/Consult;
Page 188 ~ Referral/Consult;
Page 189 ~ Referral/Consult;

Page 190 ~ Referral/Consult;
Page 191 ~ Referral/Consult;
Page 192 ~ Referral/Consult;
Page 193 ~ Referral/Consult;
Page 194 ~ Referral/Consult;
Page 195 ~ Referral/Consult;
Page 196 ~ Referral/Consult;
Page 197 ~ Referral/Consult;
Page 198 ~ Referral/Consult;
Page 200 ~ b7E;
Page 201 ~ b7E;
Page 203 ~ b5; b6; b7C; b7E;
Page 204 ~ b5;
Page 205 ~ b5;
Page 206 ~ b5;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

DECLASSIFIED BY: NSICG [redacted]
ON 07-06-2022

FD-1036 (Rev. 10-16-2009)

~~SECRET//NOFORN//LES~~

b3
b6
b7C
b7E

FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: IntelProd-LIR - Liaison Information Report **Date:** 01/22/2019

Title: (U) Cross Sector: TLP-GREEN LIR [redacted] Ghost Guns Challenge Law Enforcement

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) LIR

Synopsis: (U) Corrected LIR document attachment.

~~Reason: 1.4(c)~~
~~Derived From: Multiple Sources~~
~~Declassify On: 20441231~~

♦♦

~~SECRET//NOFORN//LES~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2022 BY [redacted] NSICG

OFFICE of PRIVATE SECTOR

b6
b7C
b7E

Liaison Information Report (LIR)
Cross-Sector

LIR [redacted]

11 January 2019

Ghost Guns Challenge Law Enforcement

The FBI's Office of Private Sector (OPS), in collaboration with the FBI Criminal Investigative (CID) and Counterterrorism (CTD) Divisions, the Department of Homeland Security (DHS), and the National Counterterrorism Center (NCTC), is providing this LIR to private sector partners to highlight the threat stemming from the use of ghost guns by criminal actors, homegrown violent extremists, and domestic extremists. Although possessing ghost guns for personal use is not a violation of federal law provided they are not for sale or distribution and the maker is not prohibited from receiving or possessing firearms, the FBI, DHS, and NCTC are concerned that the use of ghost guns in criminal or violent extremist activities will complicate law enforcement's efforts to identify the weapons used in these crimes.

Ghost guns—weapons that are not commercially manufactured and do not have serial numbers, including 3D-printed firearms—continue to pose a challenge to law enforcement, particularly when used by criminal or violent extremist actors to avoid firearms regulations and security measures. Ghost guns may be an attractive option for individuals barred from legally purchasing or possessing a firearm, or who seek to hide their activity from law enforcement. However, ghost guns are unlikely to overtake the popularity of commercially-manufactured weapons in the near term due to the availability and cost of materials, and mechanical expertise needed to manufacture them. [redacted] b7E

[redacted]

There are multiple methods to produce a ghost gun, including the use of a 3D printer, a cast mold, computer numerical control (CNC) machines, and completing a weapon with unrestricted factory-produced parts.

- 3D-Printed: The process of making a physical object from a three-dimensional digital file. 3D-printed technology has advanced rapidly in recent years and its costs have fallen. Law enforcement has seen the production of 3D-printed weapons capable of firing and receivers that are legally considered firearms. Advances in 3D-printing technology are making 3D-printed weapons more reliable and capable of being fired multiple times before catastrophic failure to the frame.

- Cast-Molded: The process in which a liquid material is poured into a mold that contains a hollow cavity of a firearm part, such as a lower receiver, and is then allowed to solidify and be broken out of the mold. Lower receivers with all necessary holes and cavities are created, meeting the legal definition of a firearm; however, the owner must also add the trigger group, hammer, upper receiver, and other components in order for the firearm to be functional. Most 80% lower receivers are cast-molded and then finished using a CNC machine with plans available on the Internet.

- Computer Numerical Control (CNC): The process of using computers to control machine tools, such as lathes, mills, and routers. CNC tools create the weapons by drilling, milling, and cutting in three dimensions to produce polymer, wood, or metal components from computer-aided design models. CNC weapons can be highly reliable, and can be as durable as commercially-manufactured firearms.

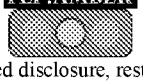
- Factory-Produced Parts: These parts are sold by a variety of Web sites and gun stores to create a functioning firearm, when combined with a lower receiver. The resulting firearm can be highly reliable and since components to build a firearm, other than the lower receiver, do not meet the legal definition of a "firearm," they are not subject to regulation or licensing.

There are numerous federal laws and regulations that apply to ghost guns. According to the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), firearms may be lawfully made by persons who do not hold a manufacturer's license provided they are not for sale or distribution and the maker is not prohibited from receiving or possessing firearms. Additionally, although markings are not required on firearms manufactured for personal use, owners are recommended to conspicuously place or engrave a serial number and/or other marks of identification to aid in investigation or recovery by state or local law enforcement officials in the event of a theft or loss of the privately owned firearm. Also, according to the ATF, plastic firearms are legal provided that after the removal of grips, stocks, and magazines, the firearm is detectable by a walk-through metal detector or an airport x-ray machine. The United States Undetectable Firearms Act of 1988 additionally requires that any firearm generate an accurate image before standard airport imaging technology. Lastly, according to the ATF, there are no restrictions on who can purchase an unfinished or 80% receiver, as they are not considered firearms.

This LIR was created and disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices

OFFICE of PRIVATE SECTOR

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

[redacted]

b3
b6
b7C
b7E

FD-1057 (Rev. 5-8-10)

UNCLASSIFIED//~~LES~~

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) FinancialServicesSector: TLP-GREEN LIR [redacted] Credit Card Skimming Expand Nationwide

Date: 01/22/2019

CC: OFFICE OF PRIVATE SECTOR

[redacted]

From: DIRECTOR'S OFFICE

Contact: [redacted]

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) LIR

(U//~~FOUO~~) [redacted] Subfile for CID Intelligence Analysis and Production.

Synopsis: (U) The Office of Private Sector's (OPS) Information Sharing and Analysis Unit (ISAU), in collaboration with the FBI's Criminal Investigative Division, produced and disseminated this Liaison Information Report (LIR) to Domestic Security Alliance Council (DSAC) and InfraGard members. The LIR informs the private sector on [redacted] Organized Groups expansion of credit card skimming at gas pumps nationwide. The authors are ISAU IA [redacted] and CID IA [redacted] The Approvers are ISAU UC [redacted] CID UC [redacted] SIAs [redacted] and reviewed by OGC [redacted] This LIR is forwarded to all PSCs via OPS Knowledge Library.

b6
b7C
b7E

Enclosure(s): Enclosed are the following items:

1. (U) LIR on [redacted] Skimmers
2. (U) SPEAR on [redacted] skimming activities

UNCLASSIFIED//~~LES~~

Title: (U) FinancialServicesSector: TLP-GREEN LIR [redacted]
Credit Card Skimming Expand Nationwide
Re: [redacted] 01/22/2019

Details:

Liaison Information Report (LIR)

Financial Services Sector

LIR [redacted] b7E

22 January 2019

[redacted] Organized Groups Expansion of Credit Card Skimming at Gas Pumps Nationwide

The FBI's Office of Private Sector, in collaboration with the FBI's Criminal Investigative Division, is providing this LIR to inform the private sector of [redacted] criminal groups' continual theft of financial data via card payment skimming activities at gas stations across the United States. Most of the skimmers are associated with [redacted] organized criminal groups. The groups use the stolen payment card data transferred from terminal modification devices or covert card readers (skimmers or shimmers) placed in gas station pumps to conduct fraudulent purchases of goods to sell at a profit. The groups have expanded their criminal activities to [redacted] (see map [redacted]

[redacted]

Some groups are interconnected; some recruit while other coerce members; some run multiple criminal schemes (such as fuel theft

or marijuana grows); others use international resources to sell goods in black markets or funnel funds through overseas accounts.

According to FBI information, **criminals have targeted** gas stations and retail stores lacking security measures, including, but not limited to, the following:

- Pumps without credit card chip technology;
- Pumps using universal keys;
- Pumps that do not require a billing zip code for sales authentication;
- Stations without surveillance cameras at gas pump areas or payment locations;
- Pumps lacking security seals; and
- Store locations with "self-checkouts" requiring neither identification nor two-factor authentication.

According to law enforcement information, the map shows [redacted]

b7E

[redacted]

Indicators of Potential Credit Card Skimming Activity

b7E

[redacted]

[redacted] b3 b7E

Title: (U) FinancialServicesSector: TLP-GREEN LIR [redacted]
Credit Card Skimming Expand Nationwide
Re: [redacted] 01/22/2019

[redacted] b7E

If you suspect you are a victim, or are aware of a skimming scheme or network, please report it to the FBI's Internet Crime Complaint Center at www.ic3.gov [please include the tag #skimming in your complaint] and/or your local FBI Field Office at https://www.fbi.gov/contact-us/field-offices.

This LIR was created and disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office:

https://www.fbi.gov/contact-us/field-offices

Title: (U) FinancialServicesSector: TLP-GREEN LIR [redacted]
Credit Card Skimming Expand Nationwide
Re: [redacted] 01/22/2019

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be

		exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
		Recipients may share TLP:

TLP:AMBER Limited disclosure, restricted to the community.	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of	Subject to standard copyright rules, TLP: WHITE information

Title: (U) FinancialServicesSector: TLP-GREEN LIR [redacted]
Credit Card Skimming Expand Nationwide
Re: [redacted] 01/22/2019

Disclosure is not limited.	misuse, in accordance with applicable rules and procedures for public release.	may be distributed without restriction.

♦♦

OFFICE of PRIVATE SECTOR

Liaison Information Report (LIR)
Financial Services Sector

LIR [redacted] b7E

22 January 2019

[redacted] Organized Groups Expansion of Credit Card Skimming at Gas Pumps Nationwide

The FBI's Office of Private Sector, in collaboration with the FBI's Criminal Investigative Division, is providing this LIR to inform the private sector of [redacted] criminal groups' continual theft of financial data via card payment skimming activities at gas stations across the United States. Most of the skimmers are associated with [redacted] organized criminal groups. The groups use the stolen payment card data transferred from terminal modification devices or covert card readers (skimmers or shimmers) placed in gas station pumps to conduct fraudulent purchases of goods to sell at a profit. The groups have expanded their criminal activities to [redacted] to avoid exposure (see map [redacted]

Some groups are interconnected; some recruit while other coerce members; some run multiple criminal schemes (such as fuel theft or marijuana grows); others use international resources to sell goods in black markets or funnel funds through overseas accounts.

[redacted]

Map: Law enforcement information [redacted]

OFFICE of PRIVATE SECTOR

According to FBI information, **criminals have targeted** gas stations and retail stores lacking security measures, including, but not limited to, the following:

- Pumps without credit card chip technology;
- Pumps using universal keys;
- Pumps that do not require a billing zip code for sales authentication;
- Stations without surveillance cameras at gas pump areas or payment locations;
- Pumps lacking security seals; and
- Store locations with "self-checkouts" requiring neither identification nor two-factor authentication.

b7E

According to law enforcement information, the map shows [redacted]

[redacted]

Indicators of Potential Credit Card Skimming Activity

The following indicators should be observed in context and not individually. These indicators include, but are not limited to, the following:

b7E

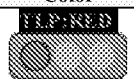
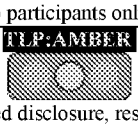
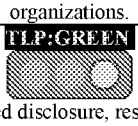
[redacted]

If you suspect you are a victim, or are aware of a skimming scheme or network, please report it to the FBI's Internet Crime Complaint Center at www.ic3.gov [please include the tag #skimming in your complaint] and/or your local FBI Field Office at https://www.fbi.gov/contact-us/field-offices.

This LIR was created and disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices

OFFICE of PRIVATE SECTOR

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
 Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
 Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
 Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DECLASSIFIED BY: NSICG
ON 07-07-2022

FD-1057 (Rev. 5-8-10)

b3
b6
b7C
b7E

~~SECRET//NOFORN~~ (U)

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) CommercialSector: TLP-GREEN LIR **Date:** 01/28/2019

CC: OFFICE OF PRIVATE SECTOR

From: DIRECTOR'S OFFICE
Contact:

b3
b6
b7C
b7E

Approved By:

Drafted By:

Case ID #: (U) LIR

(U) (S//NF)

Synopsis: (U) The FBI's International Operations Division, Counterterrorism Division, and New York Field Office, in coordination with the FBI's Office of Private Sector (OPS), produced and disseminated this Liaison Information Report (LIR) to Domestic Security Alliance Council (DSAC) and InfraGard members. The LIR inform ISAU IA reviewed/edited the LIR. Authors are IOD SIA and IA and coordinated with CTD SIA IAs

b6
b7C

~~SECRET//NOFORN~~

[redacted]

b3
b6
b7C
b7E

~~SECRET//NOFORN~~

Title: (U) CommercialSector: TLP-GREEN LIR [redacted]

[redacted]

Re: [redacted] 01/28/2019

Approvers are ISAU UC [redacted] IOD a/UC [redacted] NYO SSIA [redacted] and SIA [redacted] This LIR is forwarded to all PSCs via OPS Knowledge Library.

~~**Reason: 1.4(b)**~~
~~**Derived From: FBI NSIC CG**~~
~~**Declassify On: 20441231**~~

Enclosure(s): Enclosed are the following items:
1. (U) PDF'd LIR on [redacted] b7E

Details:

Liaison Information Report (LIR)

[redacted]

LIR [redacted]

25 January 2019

[redacted] b7E

The FBI's International Operations Division, Counterterrorism Division, and New York Field Office, in coordination with the FBI's Office of Private Sector (OPS), are providing this LIR to

[redacted] b3 b7E

~~SECRET//NOFORN~~

Title: (U) CommercialSector: TLP-GREEN LIR [redacted]

[redacted]

Re: [redacted] 01/28/2019

[redacted]

[redacted] b7E

[redacted] b7E

[redacted] b7E

~~SECRET//NOFORN~~

[redacted] b3 b7E

~~SECRET//NOFORN~~

Title: (U) CommercialSector: TLP-GREEN LIR [redacted]

[redacted]

Re: [redacted] 01/28/2019

[redacted] b7E

[redacted] b7E

[redacted] b7E

~~SECRET//NOFORN~~

[redacted] b3 b7E

~~SECRET//NOFORN~~

Title: (U) CommercialSector: TLP-GREEN LIR [redacted]

[redacted]

Re: [redacted] 01/28/2019

[redacted] b7E

This LIR was created and disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office:

https://www.fbi.gov/contact-us/field-offices

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?

Title: (U) CommercialSector: TLP-GREEN LIR [redacted]

[redacted]

Re: [redacted] 01/28/2019

TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

Title: (U) CommercialSector: TLP-GREEN LIR [redacted]

[redacted]

Re: [redacted] 01/28/2019

TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

Title: (U) CommercialSector: TLP-GREEN LIR [redacted]

[redacted]

Re: [redacted] 01/28/2019

TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

[redacted]

~~SECRET//NOFORN~~

Title: (U) CommercialSector: TLP-GREEN LIR [redacted]

[redacted]

Re: [redacted] 01/28/2019

Disclosure is not limited.	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

ENDNOTE

[redacted] b7E

[redacted]

[redacted] b3 b7E

~~SECRET//NOFORN~~

Title: (U) CommercialSector: TLP-GREEN LIR [redacted]

[redacted]

Re: [redacted] 01/28/2019

[redacted] b7E

~~SECRET//NOFORN~~

[redacted] b3 b7E

~~SECRET//NOFORN~~

Title: (U) CommercialSector: TLP-GREEN LIR [redacted]

[redacted]

Re: [redacted] 01/28/2019

[redacted] b7E

~~SECRET//NOFORN~~

[redacted]

b3
b7E

~~SECRET//NOFORN~~

Title: (U) CommercialSector: TLP-GREEN LIR [redacted]

[redacted]

Re: [redacted] 01/28/2019

[redacted]

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-07-2022 BY [redacted]
b6
b7C

TLP:GREEN

OFFICE of PRIVATE SECTOR

Liaison Information Report (LIR)
Commercial Facilities Sector
Hospitality and Tourism Industry

LIR [redacted] b7E

25 January 2019

[redacted]

b7E

OFFICE of PRIVATE SECTOR

b7E

This LIR was created and disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices

OFFICE of PRIVATE SECTOR

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

[redacted]

b3
b6
b7C
b7E

FD-1057 (Rev. 5-8-10)

UNCLASSIFIED//~~LES~~

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) Financial Sector: TLP - Green LIR [redacted] on Fraudulent Hedge Funds **Date:** 01/29/2019

CC: OFFICE OF PRIVATE SECTOR
[redacted]

From: DIRECTOR'S OFFICE
Contact: [redacted]

Approved By: UC [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) LIR

(U//~~LES~~) Corporate and Securities /Commodities Fraud - [redacted]
(U//~~LES~~) MONEY LAUNDERING FACILITATION THREAT;
[redacted]

Synopsis: (U) (U) The FBI's New York Office, and Criminal Investigative Division, in coordination with the FBI's Office of Private Sector (OPS), produced and disseminated this Liaison Information Report (LIR) to Domestic Security Alliance Council (DSAC) and InfraGard members. The LIR inform the financial services sector. ISAU IA [redacted] reviewed/edited the LIR. Authors are New York Office and Criminal Investigative Division. Approvers are ISAU UC [redacted] NYO SIA [redacted] SIA [redacted] CID UC [redacted] This LIR is forwarded to all PSCs via OPS Knowledge Library.

Enclosure(s): Enclosed are the following items:
1. (U) LIR

UNCLASSIFIED//~~LES~~

[redacted] b3 b7E

UNCLASSIFIED//~~LES~~

Title: (U) Financial Sector: TLP - Green LIR [redacted] on Fraudulent Hedge Funds
Re: [redacted] 01/29/2019

Details:

Liaison Information Report (LIR)

Financial Services Sector

LIR [redacted] b7E

29 January 2019

Financial Crime Threat Actors Very Likely Laundering Illicit Proceeds Through Fraudulent Hedge Funds and Private Equity Firms to Obfuscate Illicit Proceeds

FBI New York, in coordination with the Criminal Investigative Division and the Office of the Private Sector, assess financial crime threat actors very likely launder illicit proceeds from financial fraud schemes through fraudulent hedge funds[a] and private equity firms[b] to obfuscate illicit proceeds. The use of fraudulent hedge funds and private equity firms provide financial crime threat actors with access to a pool of high net wealth individuals along with connections to the international financial system, which very likely assists in the perpetration of financial crime schemes and money laundering.

Title: (U) Financial Sector: TLP - Green LIR [redacted] on Fraudulent Hedge Funds

Re: [redacted] 01/29/2019

If you notice or become aware of any such activity, contact your local FBI field office. Remain vigilant as well as routinely train personnel on suspicious activity indicators and reporting procedure.

[redacted]

[redacted] b3 b7E

Title: (U) Financial Sector: TLP - Green LIR [redacted] on Fraudulent Hedge Funds

Re: [redacted] 01/29/2019

[redacted] b7D b7E

FBI NY assesses additional financial crime threat actors will likely embrace the use of fraudulent hedge funds and private equity firms to obfuscate the movement of illicit funds. The increased use of fraudulent hedge funds and private equity firms will likely be driven by the access these entities provide to move large amounts of illicit proceeds and to avoid detailed financial regulatory reporting. If financial crime threat actors increase their use of fraudulent hedge funds and private equity firms to launder illicit funds, FBI NY would expect an increase in private adviser exemptions to the SEC, an increase in the industry pools of assets under management held by hedge funds and private equity firms, and a possible decrease in other money laundering techniques, to include bulk cash smuggling and the use of money mules. FBI NY assesses if additional financial crime threat actors use fraudulent hedge funds and private equity firms to launder illicit proceeds, there will likely be an increase in financial losses to this wealth management sector prompting greater regulatory oversight.

Title: (U) Financial Sector: TLP - Green LIR [redacted] on Fraudulent Hedge Funds

Re: [redacted] 01/29/2019

This LIR was created and disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office.

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure,	Sources may use TLP:RED when information cannot be effectively acted upon by additional	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context

restricted to participants only.	parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared	Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are**

Title: (U) Financial Sector: TLP - Green LIR [redacted] on Fraudulent Hedge Funds

Re: [redacted] 01/29/2019

	outside of the organizations involved.	**at liberty to specify additional intended limits of the sharing: these must be adhered to.**
[redacted] Limited disclosure, restricted to the community.	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be

		released outside of the community.
Disclosure is not limited.	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

Traffic Light Protocol (TLP) Definitions

Title: (U) Financial Sector: TLP - Green LIR [redacted] on Fraudulent Hedge Funds

Re: [redacted] 01/29/2019

[a] (U) A hedge fund is an alternative investment vehicle available only to sophisticated investors, such as institutions and individuals with significant assets. Like mutual funds, hedge funds are pools of underlying securities. *(Web site;*

INVESTOPEDIA; "Hedge Fund"; 2018; http://www.investopedia.com/terms/h /hedgefund.asp; accessed on 15

October 2018; The source is a website that compiles financial services information.)

[b] (U) A private equity firm is an investment vehicle which invests directly in companies, primarily by purchasing private companies; although, it sometimes seeks to acquire controlling interest in publicly-traded companies through stock purchases. Private equity firms frequently use leveraged buyouts to acquire financially distressed companies. *(Web site; INVESTOPEDIA; "Private Equity"; 2018; http://www.investopedia.com/terms/p/privateequity.asp;*

accessed on 15 October 2018; The source is a website that compiles financial services information.)

[c] (U) Cryptocurrency is a math-based, decentralized convertible virtual currency that is protected by cryptography. Cryptocurrency incorporates principles of cryptography to implement a distributed, decentralized, secure information economy. It relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred. *(Web site; INVESTOPEDIA; "Cryptocurrency"; 2018; http://www.investopedia.com/terms/c/cryptocurrency.asp; accessed on 17 October 2018;*

The source is a website that compiles financial services information.)

[1] (U) FBI; FD-302; [redacted] 11 September 2018; 4 September 2018; "(U) Search of [redacted]"; UNCLASSIFIED; UNCLASSIFIED; Reporting comes from financial documents as obtained through the course of an FBI investigation.

[2] (U) FBI; FD-1057; [redacted] 26 December 2018; 3 October 2018; "(U) Interview of [redacted] UNCLASSIFIED; UNCLASSIFIED; Reporting comes from a human source with excellent access.

[3] (U) FBI; FD-302; [redacted] 20 December 2018; 6 December 2018; (U) Custodial Interview of [redacted] UNCLASSIFIED; UNCLASSIFIED; Reporting comes from a human source with excellent access.

♦♦

OFFICE of PRIVATE SECTOR

Liaison Information Report (LIR)
Financial Services Sector

LIR [redacted] b7E

29 January 2019

Financial Crime Threat Actors Very Likely Laundering Illicit Proceeds Through Fraudulent Hedge Funds and Private Equity Firms to Obfuscate Illicit Proceeds

FBI New York, in coordination with the Criminal Investigative Division and the Office of the Private Sector, assess financial crime threat actors very likely launder illicit proceeds from financial fraud schemes through fraudulent hedge funds[a] and private equity firms[b] to obfuscate illicit proceeds. The use of fraudulent hedge funds and private equity firms provide financial crime threat actors with access to a pool of high net wealth individuals along with connections to the international financial system, which very likely assists in the perpetration of financial crime schemes and money laundering.

If you notice or become aware of any such activity, contact your local FBI field office. Remain vigilant as well as routinely train personnel on suspicious activity indicators and reporting procedure.

[redacted] b7D b7E

[a] A hedge fund is an alternative investment vehicle available only to sophisticated investors, such as institutions and individuals with significant assets. Like mutual funds, hedge funds are pools of underlying securities.

[b] A private equity firm is an investment vehicle which invests directly in companies, primarily by purchasing private companies; although, it sometimes seeks to acquire controlling interest in publicly-traded companies through stock purchases. Private equity firms frequently use leveraged buyouts to acquire financially distressed companies.

[c] Cryptocurrency is a math-based, decentralized convertible virtual currency that is protected by cryptography. Cryptocurrency incorporates principles of cryptography to implement a distributed, decentralized, secure information economy. It relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred.

OFFICE of PRIVATE SECTOR

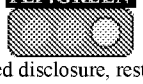
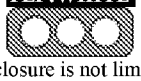
b7D
b7E

FBI NY assesses additional financial crime threat actors will likely embrace the use of fraudulent hedge funds and private equity firms to obfuscate the movement of illicit funds. The increased use of fraudulent hedge funds and private equity firms will likely be driven by the access these entities provide to move large amounts of illicit proceeds and to avoid detailed financial regulatory reporting. If financial crime threat actors increase their use of fraudulent hedge funds and private equity firms to launder illicit funds, FBI NY would expect an increase in private adviser exemptions to the SEC, an increase in the industry pools of assets under management held by hedge funds and private equity firms, and a possible decrease in other money laundering techniques, to include bulk cash smuggling and the use of money mules. FBI NY assesses if additional financial crime threat actors use fraudulent hedge funds and private equity firms to launder illicit proceeds, there will likely be an increase in financial losses to this wealth management sector prompting greater regulatory oversight.

This LIR was created and disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office.

OFFICE of PRIVATE SECTOR

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

[redacted]

b3
b6
b7C
b7E

FD-1057 (Rev. 5-8-10)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) TLP Green Cross-Sector LIR [redacted] **Date:** 02/12/2019

[redacted]

CC: [redacted]

From: DIRECTOR'S OFFICE

Contact: [redacted]

b3
b6
b7C
b7E

Approved By: UC [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) LIR

(U) Weapons of Mass Destruction;

[redacted]

Synopsis: (U) The FBI's Weapons of Mass Destruction Directorate, in coordination with the Office of Private Sector (OPS), is providing this LIR to inform private sector partners of open source reports describing the receipt by [redacted] The LIR will be disseminated to Domestic Security Alliance Council (DSAC) and InfraGard members. ISAU IA [redacted] reviewed the LIR. The author is WMD IA [redacted] The approvers are ISAU UC [redacted] CBIU UC [redacted] WMD SIA [redacted] and forwarded to all PSCs.

b6
b7C
b7E

Administrative Notes: (U) TLP Green LIR [redacted]

Package Copy: (U) N/A

Enclosure(s): Enclosed are the following items:

UNCLASSIFIED

[redacted] b3 b7E

Title: (U) TLP Green Cross-Sector LIR [redacted]

Re: [redacted] 02/12/2019

1. (U) TLP Green Cross-Sector LIR [redacted]

Details:

Liaison Information Report (LIR)

Cross Sector

LIR [redacted] b7E

04 February 2019

[redacted] b7E

The FBI's Weapons of Mass Destruction Directorate, in coordination with the Office of Private Sector (OPS), is providing this LIR to inform private sector partners of open source reports describing the receipt by [redacted]

[redacted]

[redacted] b3 b7E

Title: (U) TLP Green Cross-Sector LIR [redacted]

[redacted]

Re: [redacted], 02/12/2019

b7E

[redacted]

The FBI's Office of Private Sector and the Weapons of Mass Destruction Directorate respectfully request feedback or information if your company is aware of any incidents of similar nature.

[redacted] b7E

Title: (U) TLP Green Cross-Sector LIR [redacted]

Re: [redacted] 02/12/2019

Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices.

Color	When should it be used?	How may it be shared?

Title: (U) TLP Green Cross-Sector LIR [redacted]

Re: [redacted] 02/12/2019

TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

Title: (U) TLP Green Cross-Sector LIR [redacted]

Re: [redacted] 02/12/2019

TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

Title: (U) TLP Green Cross-Sector LIR [redacted]

Re: [redacted] 02/12/2019

TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

[redacted] b3 b7E

Title: (U) TLP Green Cross-Sector LIR [redacted]

Re: [redacted] 02/12/2019

Disclosure is not limited.	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

Traffic Light Protocol (TLP) Definitions

[redacted] b7E

[redacted]

Title: (U) TLP Green Cross-Sector LIR [redacted]

Re: [redacted] 02/12/2019

[redacted]

♦♦

OFFICE of PRIVATE SECTOR

Liaison Information Report (LIR)
Cross Sector

LIR [redacted] b7E

04 February 2019

[redacted]

The FBI's Weapons of Mass Destruction Directorate, in coordination with the Office of Private Sector (OPS), is providing this LIR to inform private sector partners of open source reports describing the receipt by [redacted]

[redacted]

The FBI's Office of Private Sector and the Weapons of Mass Destruction Directorate respectfully request feedback or information if your company is aware of any incidents of similar nature.

OFFICE of PRIVATE SECTOR

This LIR was created and disseminated from the Weapons of Mass Destruction Directorate and OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices.

OFFICE of PRIVATE SECTOR

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

[redacted]

b3
b6
b7C
b7E

FD-1057 (Rev. 5-8-10)

UNCLASSIFIED//~~FOUO~~

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) CrossSector: TLP-GREEN LIR [redacted] **Date:** 02/12/2019

[redacted]

CC: OFFICE OF PRIVATE SECTOR

[redacted]

From: DIRECTOR'S OFFICE

Contact: [redacted]

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) LIR

(U//~~FOUO~~) [redacted]

ASSESSMENT FILE;

[redacted]

COUNTERTERRORISM DIVISION;

Synopsis: (U) The FBI's Counterterrorism Division, in coordination with the FBI's Office of Private Sector (OPS), produced and disseminated this Liaison Information Report (LIR) to Domestic Security Alliance Council and InfraGard members. The LIR inform

[redacted]

b6
b7C
b7E

ISAU IA [redacted]

Authors are CTD/CTHS SIA [redacted]

UNCLASSIFIED//~~FOUO~~

[redacted]

b3
b6
b7C
b7E

Title: (U) CrossSector: TLP-GREEN LIR [redacted]

Re: [redacted] 02/12/2019

[redacted] Approvers are ISAU UC [redacted] and CTD UC [redacted] This LIR is forwarded to all PSCs via OPS Knowledge Library.

Enclosure(s): Enclosed are the following items:
1. (U) LIR

Details:

Liaison Information Report (LIR)

Cross Sector

[redacted] b7E

12 February 2019

[redacted] b7E

The FBI's Counterterrorism Division (CTD), in coordination with the FBI's Office of Private Sector (OPS), is providing this LIR to [redacted]

[redacted]

Title: (U) CrossSector: TLP-GREEN LIR [redacted]

[redacted]

Re: [redacted] 02/12/2019

[redacted]

[redacted]

[redacted]

[redacted] b7E

[redacted]

Title: (U) CrossSector: TLP-GREEN LIR

Re: 02/12/2019

[redacted] b3 b7E

Title: (U) CrossSector: TLP-GREEN LIR [redacted]

Re: [redacted] 02/12/2019

[redacted] b7E

Solution Discussions

[redacted] b7E

Title: (U) CrossSector: TLP-GREEN LIR

Re: 02/12/2019

This LIR was created and disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office:

https://www.fbi.gov/contact-us/field-offices

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?

TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
		Recipients may only

TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
	Sources may use TLP: GREEN when	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or

~~TLP:GREEN~~ Limited disclosure, restricted to the community.	information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
Disclosure is not limited.	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and	Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

	procedures for public release.	

ENDNOTE

[3] (U)

[redacted] b3 b7E

Title: (U) CrossSector: TLP-GREEN LIR [redacted]

Re: [redacted] 02/12/2019

b7E

[redacted]

[redacted] b3 b7E

Title: (U) CrossSector: TLP-GREEN LIR [redacted]

Re: [redacted] 02/12/2019

[redacted] b7E

[redacted] b3 b7E

Title: (U) CrossSector: TLP-GREEN LIR [redacted]

Re: [redacted] 02/12/2019

[redacted] b7E

♦♦

OFFICE of PRIVATE SECTOR

Liaison Information Report (LIR)
Cross Sector

LIR [redacted] b6 b7C b7E

12 February 2019

[redacted]

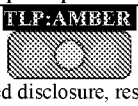
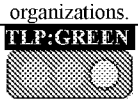
OFFICE of PRIVATE SECTOR

b7E

This LIR was disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices

OFFICE of PRIVATE SECTOR

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

[redacted]

b3
b6
b7C
b7E

FD-1057 (Rev. 5-8-10)

UNCLASSIFIED//~~FOUO~~

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) Healthcare Sector, TLP: GREEN, LIR [redacted]– Robbery Crews Targeting 24-Hour Pharmacies **Date:** 02/15/2019

CC: OFFICE OF PRIVATE SECTOR
OPS-SC (SC)

From: DIRECTOR'S OFFICE
Contact: [redacted]

Approved By: UC [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) LIR

(U//~~FOUO~~) [redacted]

Synopsis: (U) TLP:GREEN FBI Baltimore, in coordination with Office of Private Sector, prepared this LIR to inform the Healthcare and Public Health sector about the concerning number of robberies targeting 24-hour retail pharmacies throughout the United States. ISAU IA [redacted] and IAC CDC [redacted] ADC [redacted] (BA) reviewed the LIR, the author was IA [redacted] (BA), and the approvers were SIA [redacted] SSA [redacted] SSA [redacted] ASAC [redacted] ASAC [redacted] and ISAU UC [redacted]

b6
b7C

Enclosure(s): Enclosed are the following items:
1. (U) FBI Baltimore, in coordination with Office of Private Sector, prepared this LIR to inform the Healthcare and Public Health sector about the concerning number of robberies targeting 24-hour retail pharmacies throughout the United States.

Details:

TLP: GREEN

UNCLASSIFIED//~~FOUO~~

Title: (U) Healthcare Sector, TLP: GREEN, LIR [redacted] - Robbery Crews Targeting 24-Hour Pharmacies
Re: [redacted] 02/15/2019

Liaison Information Report (LIR)

Healthcare and Public Health Sector

08 February 2019 LIR [redacted] b7E

Robbery Crews Targeting 24-Hour Pharmacies for Controlled Prescription Drugs

FBI Baltimore, in coordination with Office of Private Sector, prepared this LIR to inform the Healthcare and Public Health sector about the concerning number of robberies targeting 24-hour retail pharmacies throughout the United States. FBI information indicates retail pharmacy locations open 24-hours represent attractive targets for robbery crews seeking to obtain controlled prescription drugs, both for personal use and street market resale, given the large profits commanded by the illicit sale of controlled prescription drugs.

Most 24-hour pharmacies are run by major pharmacy chains, which offer extended hours and typically hold larger inventories of controlled prescription drugs than independent pharmacies. Robbery crews target 24-hour pharmacies in late evening and early morning, likely due to light staffing of pharmacies, fewer customers, and less congested roadways when fleeing robbery locations. Robbery crews' targeting of 24-hour pharmacies may be driven by knowledge of past successful robberies and familiarity with store layouts and security measures.

Retail pharmacy locations will remain desirable targets for robbery crews seeking to obtain controlled prescription drugs. Efforts by retail pharmacies to enhance visible security measures—adding armed guards, glass partition walls over pharmacy counters, security cameras, and high definition in-store security monitors—may deter would-be robbers. The installation of time-delayed safes in pharmacies contributes to a decrease in robberies for controlled prescription

drugs. Equally important are adequate staffing levels, and employees who are alert, greet customers who enter the store, and are well trained on how to react during and after pharmacy robberies.

Security measures suggested by law enforcement include [redacted]

b7E

[redacted]

[redacted]

[redacted] b3 b7E

Title: (U) Healthcare Sector, TLP: GREEN, LIR [redacted] - Robbery Crews Targeting 24-Hour Pharmacies
Re: [redacted] 02/15/2019

[redacted] b7E

This LIR was disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices.

TLP: GREEN

♦♦

OFFICE of PRIVATE SECTOR

Liaison Information Report (LIR)
Healthcare and Public Health Sector

08 February 2019 LIR [redacted] b7E

Robbery Crews Targeting 24-Hour Pharmacies for Controlled Prescription Drugs

FBI Baltimore, in coordination with Office of Private Sector, prepared this LIR to inform the Healthcare and Public Health sector about the concerning number of robberies targeting 24-hour retail pharmacies throughout the United States. FBI information indicates retail pharmacy locations open 24-hours represent attractive targets for robbery crews seeking to obtain controlled prescription drugs, both for personal use and street market resale, given the large profits commanded by the illicit sale of controlled prescription drugs.

Most 24-hour pharmacies are run by major pharmacy chains, which offer extended hours and typically hold larger inventories of controlled prescription drugs than independent pharmacies. Robbery crews target 24-hour pharmacies in late evening and early morning, likely due to light staffing of pharmacies, fewer customers, and less congested roadways when fleeing robbery locations. Robbery crews' targeting of 24-hour pharmacies may be driven by knowledge of past successful robberies and familiarity with store layouts and security measures.

Retail pharmacy locations will remain desirable targets for robbery crews seeking to obtain controlled prescription drugs. Efforts by retail pharmacies to enhance visible security measures—adding armed guards, glass partition walls over pharmacy counters, security cameras, and high definition in-store security monitors—may deter would-be robbers. The installation of time-delayed safes in pharmacies contributes to a decrease in robberies for controlled prescription drugs. Equally important are adequate staffing levels, and employees who are alert, greet customers who enter the store, and are well trained on how to react during and after pharmacy robberies.

Security measures suggested by law enforcement include the [redacted] b7E

[redacted]

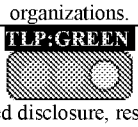
OFFICE of PRIVATE SECTOR

b7E

This LIR was disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices.

OFFICE of PRIVATE SECTOR

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

[redacted]

b3
b6
b7C
b7E

FD-1036 (Rev. 10-16-2009)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: IntelProd-LIR - Liaison Information Report **Date:** 02/28/2019

Title: (U) Financial Sector: TLP - Green LIR [redacted] on Fraudulent Hedge Funds

Approved By: UC [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) LIR

Synopsis: (U) DUPLICATE (Serial 78) - The FBI's New York Office, and Criminal Investigative Division, in coordination with the FBI's Office of Private Sector (OPS), produced and disseminated this Liaison Information Report (LIR) to Domestic Security Alliance Council (DSAC) and InfraGard members. The LIR inform the financial services sector. ISAU IA [redacted] reviewed/edited the LIR. Authors are New York Office and Criminal Investigative Division . Approvers are ISAU UC [redacted] NYO SIA [redacted] SIA [redacted] CID UC [redacted] This LIR is forwarded to all PSCs via OPS Knowledge Library.

b6
b7C

♦♦

UNCLASSIFIED

[redacted]

b3
b6
b7C
b7E

FD-1036 (Rev. 10-16-2009)

UNCLASSIFIED//~~FOUO~~

FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: IntelProd-LIR - Liaison Information Report **Date:** 02/28/2019

Title: (U) LIR [redacted] Robbery Crews Targeting 24-Hour Pharmacies for Controlled Prescription Drugs

Approved By: UC [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) LIR

(U//~~FOUO~~) Intelligence Products Published under Violent Incident Crimes [redacted]

Synopsis: (U) FBI Baltimore, in coordination with Office of Private Sector, prepared this LIR to inform the Healthcare and Public Health sector about the concerning number of robberies targeting 24-hour retail pharmacies throughout the United States. FBI information indicates retail pharmacy locations open 24-hours represent attractive targets for robbery crews seeking to obtain controlled prescription drugs, both for personal use and street market resale, given the large profits commanded by the illicit sale of controlled prescription drugs.

♦♦

[redacted]

b3
b6
b7C
b7E

FD-1036 (Rev. 10-16-2009)

UNCLASSIFIED//~~FOUO~~

FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: IntelProd-LIR - Liaison Information Report **Date:** 02/28/2019

Title: (U) LIR [redacted] Indiana Based Crew Conducting Armed Pharmacy Robberies, TLP-GREEN, Healtcare

Approved By: UC [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) LIR

(U) [redacted] (Subjects);
Multiple Pharmacies Throughout the United States (Victims);
Hobbs Act - Commercial Institutions;
OO: IP

Synopsis: (U) The FBI Indianapolis Field Office (IP) and the Criminal Investigative Division (CID), in coordination with the Office of Private Sector's (OPS) Information Sharing and Analysis Unit (ISAU), prepared this Liaison Information Report (LIR) and, upon approval, ISAU will be disseminating it to Domestic Security Alliance Council (DSAC) and InfraGard members. The LIR informs the private sector that a group of individuals has been identified as either orchestrating, or participating in, an ongoing series of pharmacy robberies in 16 states. ISAU IA [redacted] CDC [redacted] (IP), ADC [redacted] (IP) reviewed the LIR. The authors were IA [redacted] (IP) and IA [redacted] (CID). The approvers were SIA [redacted] (IP), SIA [redacted] (IP), SSA [redacted] (IP), A/ASAC [redacted] UC [redacted] (CID), and ISAU UC [redacted] This LIR will be forwarded to all PSCs via OPS Knowledge Library.

b6
b7C

♦♦

UNCLASSIFIED//~~FOUO~~

OFFICE of PRIVATE SECTOR

Liaison Information Report (LIR)
Healthcare and Public Health Sector
Pharmaceutical Industry

30 November 2018

LIR [redacted] b7E

Indiana Based Crew Conducting Armed Pharmacy Robberies throughout the United States, as of October 2018

The FBI Indianapolis Field Office and the Criminal Investigative Division (CID), in coordination with the Office of Private Sector (OPS), prepared this LIR to inform private sector partners that a group of individuals has been identified as either orchestrating, or participating in, an ongoing series of pharmacy robberies in 16 states.

Between November 2017 and October 2018, this robbery crew has been linked to 36 robberies taking place in:

❖ Arkansas	❖ Georgia	❖ Illinois	❖ Indiana
❖ Iowa	❖ Kansas	❖ Kentucky	❖ Louisiana
❖ Massachusetts	❖ Michigan	❖ Minnesota	❖ Missouri
❖ Nebraska	❖ Pennsylvania	❖ Tennessee	❖ Wisconsin

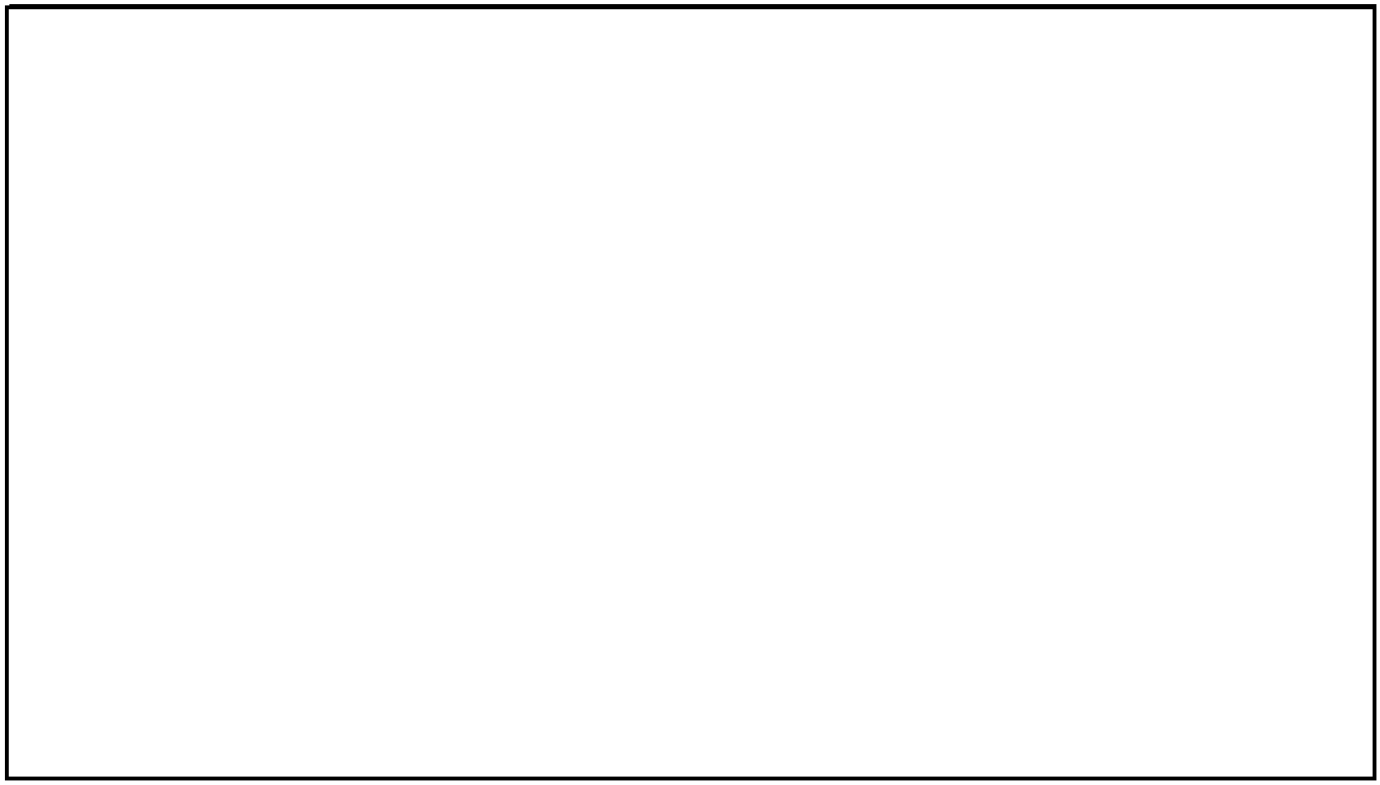
The modus operandi of these pharmacy robberies include the following:

[redacted] b7E

OFFICE of PRIVATE SECTOR

Indiana Based Crew Conducting Armed Pharmacy Robberies throughout the United States:

b7E



Note: All 36 known robberies committed between November 2017 and October 2018.

This LIR was created and disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices

OFFICE of PRIVATE SECTOR

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

[redacted] b3 b7E

FD-1036 (Rev. 10-16-2009)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: IntelProd-LIR - Liaison Information Report **Date:** 02/28/2019

Title: (U) GovtFacilities: TLP-WHITE LIR [redacted]-Unknown Fraud Actors Conducting ACH Scams

Approved By: [redacted] b3 b6 b7C b7E

Drafted By: [redacted]

Case ID #: [redacted] (U) LIR

196D-WF-2994604-INTELPRODS

(U) [redacted] Fairfax County Government Director of Finance - Victim; Other - Wire and Mail Fraud Schemes

[redacted]

(U) INTELLIGENCE ANALYSIS AND PRODUCTION - CRIMINAL

(U) INTELLIGENCE DIVISION BRIEFING /LIAISON - CRIMINAL

Synopsis: (U) The FBI's Washington Field Office, in coordination with the FBI's Office of Private Sector (OPS), produced and disseminated this Liaison Information Report (LIR) to Domestic Security Alliance Council and InfraGard members. The LIR inform public and private sector entities about Automated Clearing House fraud schemes being conducted throughout the United States. ISAU IA [redacted] reviewed/edited the LIR. The author is WFO IA [redacted] b6 b7C b7E Approvers are ISAU UC [redacted] WFO a/ASAC [redacted] SSIAs [redacted] SIA [redacted] SSA [redacted] This LIR is forwarded to all PSCs via OPS Knowledge Library.

Disseminated product does not have endnotes. Source is SIR-[redacted] referenced.

♦♦

UNCLASSIFIED

OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

GOVERNMENT FACILITIES SECTOR

28 February 2019

LIR [ ] b7E

Unknown Fraud Actors Conducting ACH Scams Against the Private and Public Sector Throughout the United States

The FBI's Washington Field Office, in coordination with the FBI's Office of Private Sector (OPS), prepared this LIR to inform public and private sector entities about Automated Clearing House (ACH) fraud schemes being conducted throughout the United States. FBI information indicates unknown fraud actors have contacted local government or academic institutions alleging to represent legitimate vendors and submitting fraudulent ACH forms to redirect contract payments to fraudulent bank accounts.

Notable Indicators

- Some of the fraudulent emails stated, "We have attached a new (local government or state name) Vendor ACH Authorization form. Please update our banking data to reflect the new information."
- The signature had the legitimate name of the person at the vendor company with the title "Contract Administrator" then "Government Accounts" directly under.
- The commonality of the email addresses used in multiple schemes was the first and last name of a legitimate person at the vendor company "@gmx.com", "@yandex.com", or "@mail.com."

The Scheme Details

Since May 2018, multiple local governments have received emails with ACH change of payment forms from imposter email addresses that the local governments believed were legitimately associated with third party vendors. The actor(s) used a name to impersonate an individual employed at the legitimate third party vendor's organization. The actor(s) frequently impersonated computer, construction, and internet service provider vendors. The actor(s) accessed publically available ACH change of payment forms on each of the local government's websites and emailed the form to the point of contact listed. The local governments or academic institutions implemented the changes as instructed and subsequently made payments to the perpetrators' bank accounts.

The actor(s) are known to re-victimize institutions by impersonating as another vendor. Public sector and academia partners should remain vigilant in safeguarding sensitive ACH and vendor information from public access, report any suspicious activities to their security department, local law enforcement, and the FBI:

- The FBI Tip Website www.FBI.gov/tips
- The FBI Internet Crime Complaint Center (IC3) www.ic3.gov
- The FBI CyWatch at: cywatch@ic.fbi.gov – or – 855-292-3937

This LIR was disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices

Disclosure is Not Limited

OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

[redacted] b3 b7E

FD-1036 (Rev. 10-16-2009)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: IntelProd-LIR - Liaison Information Report **Date:** 03/12/2019

Title: (U) [redacted] b3 b6 b7C b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) LIR

258A-DE-2461507-INTELPRODS (U) Intelprods sub-file.

Synopsis: (U) The FBI's Office of Private Sector (OPS), in collaboration with the FBI's Detroit Field Office, produced and disseminated this Liaison Information Report (LIR) to Domestic Security Alliance Council and InfraGard members. [redacted] The authors are ISAU IA [redacted] and DE IA [redacted] Approvers are ISAU UC [redacted] DE IPC [redacted] SIA [redacted] and SSRA [redacted] This LIR is forwarded to all PSCs via OPS Knowledge Library. Disseminated product does not have endnotes. Source is referenced DE SIR-[redacted] b6 b7C b7E

♦♦

UNCLASSIFIED

DECLASSIFIED BY: NSICG
ON 07-06-2022

b3
b6
b7C
b7E

FD-1036 (Rev. 10-16-2009)

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: IntelProd-LIR - Liaison Information Report **Date:** 03/12/2019

Title: (U) Cross Sector: TLP-WHITE LIR [redacted] Indictment of Monica Witt Highlights Espionage Threat

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) LIR

(U) ~~(S//NF)~~ ESPIONAGE

Synopsis: (U) The FBI's Counterintelligence Division, in coordination with the FBI's Office of Private Sector (OPS), produced and disseminated this Liaison Information Report (LIR) to Domestic Security Alliance Council and InfraGard members. The LIR provide the private sector partners information regarding insider threat and foreign intelligence services' recruitment efforts against the United States. ISAU IA [redacted] reviewed/edited the LIR. The author is CD IA [redacted] Approvers are ISAU UC [redacted] CD DAD Nikki L. Floris, and UC [redacted] and SIA [redacted] and reviewed by OGC [redacted] This LIR is forwarded to all PSCs via OPS Knowledge Library. Disseminated product does not have endnotes (PDF version with endnotes also attached). Sources are U.S. DOJ Press Releases.

b6
b7C

Enclosure(s): Enclosed are the following items:

1. (U) Draft LIR with Endnotes - DOJ press releases citations.

~~**Reason: 1.4(b)**~~
~~**Derived From: FBI NSIC CG**~~
~~**Declassify On: 20441231**~~

♦♦

~~SECRET//NOFORN~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-06-2022 BY [redacted] NSICG

b6
b7C
b7E

OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

CROSS SECTOR

12 March 2019 **LIR** [redacted]

Indictment of Monica Witt Highlights Espionage Threat

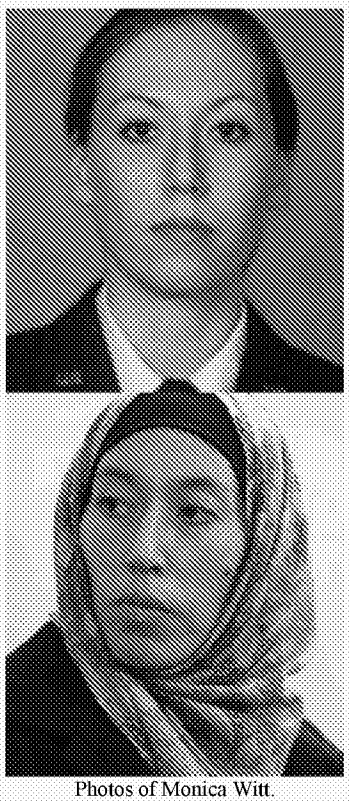
The FBI's Counterintelligence Division, in coordination with the FBI's Office of Private Sector (OPS), is providing information regarding insider threat and foreign intelligence services' (FIS's) recruitment efforts against the United States. FIS consider individuals who have jobs in sensitive military and civilian areas of special interest. The mainstay of most intelligence services worldwide is the recruitment of well-placed assets who can provide insightful information addressing their intelligence/information needs. FIS use elicitation, recruitment, physical, and cyber-based operations to conduct their clandestine collection activities. Volunteers[a], who offer sensitive information freely, represent a notable risk to corporations' data loss, and a threat to US national security.

The Threat from One of the US Government's Own

On 13 February 2019, the FBI, in conjunction with the US Department of Justice (DOJ) and the US Department of Treasury, unsealed an indictment against a US citizen, Monica Witt on charges of espionage, including the transmittal of national defense information to the Government of Iran (GOI). Witt is a former active duty US Air Force Intelligence Specialist and Special Agent for the Air Force Office of Special Investigation. Between 1997 and 2008, she served continuously in the military before working as a US Government (USG) contractor until 2010. Her military service and contracting employment provided her access to SECRET and TOP SECRET information relating to foreign intelligence and counterintelligence, including the true names of US Intelligence Community undercover personnel. In 2013, she defected to Iran.

- In August 2013, Witt traveled to Iran after declaring herself to GOI officials as a US military veteran who desired to defect to Iran. Witt subsequently provided information to the GOI, placing at risk sensitive and classified US national defense information and programs.

- Witt intentionally provided information endangering USG personnel and their families stationed abroad. Witt conducted research on behalf of the GOI, for the purpose of drafting "target packages" against former colleagues within the USG.



Photos of Monica Witt.

Source: DOJ; 13 February 2019

[a] A **volunteer** is an individual who initiates contact with a foreign government, often by calling, e-mailing, or walking into a foreign diplomatic establishment, to clandestinely provide national defense information he/she is unauthorized to share, usually in exchange for money or other compensation.

- Witt's defection to Iran has benefited the Islamic Revolutionary Guard Corps (IRGC), which has elements responsible for intelligence collection, unconventional warfare, and providing direct support to multiple terrorist organizations targeting US citizens and interests.

- Before her defection, Witt traveled to Iran to attend IRGC-sponsored propaganda events and conferences, whose stated goal is condemning American moral standards and promoting anti-US propaganda. Witt appeared in multiple Iranian propaganda videos in which she was identified as a US veteran and made statements critical of the USG and military.

Possible Indicators of an Insider Threat

These are indicators that should be observed in context and not individually. The identified suspicious circumstances or behaviors below may not indicate an individual is committing espionage. However, a combination of factors highlight a need for further investigation to determine whether an insider threat and risk to your company and/or the Nation's sensitive information exist.

- Undisclosed Foreign Contacts
- Undisclosed Foreign Travel
- Excessive/Unusual Foreign Travel
- Failure to Report Offer of Financial Assistance by Foreign National
- Failure to Report Requests for Proprietary, Classified, or Other Sensitive Information
- Unreported Relationship with a Foreign Government or Intelligence Service
- Exercising Benefits of Dual Citizenship
- Unjustified Work Pattern (Late Nights, Weekends, etc.)
- Improperly Removing Sensitive or Classification Markings on Documents or Media
- Discussing Classified Information on Non-secure Phones or Email
- Attempting to Discuss or Gain Access to Sensitive Information of Programs without Business Need
- Repetitive Violations of Organizational Protocol and Policies
- Behavior Suggests Allegiance to Foreign Entity
- Unexplained Affluence

This LIR was disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office:
https://www.fbi.gov/contact-us/field-offices

OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Official Record

FEDERAL BUREAU OF INVESTIGATION

Import Form

Form Type: [redacted] LIR - Liaison Information Report **Date:** 05/23/2019 b7E

Title: (U) Federal Hunting License Exception Could Be Exploited by Extremists or Criminal Actors Seeking t

Approved By: [redacted] b6 b7C

Drafted By: [redacted]

Case ID #: [redacted] (U) LIR b3 b7E

(U//~~FOUO~~) [redacted]

Synopsis: (U) The FBI's Office of Private Sector (OPS), in collaboration with the FBI Counterterrorism Division (CTD), is providing this LIR to private sector partners to highlight our concern that extremists and other criminal actors could exploit the federal statutory exception that allows non-immigrant visa holders—who are otherwise prohibited from shipping, transporting, receiving, or possessing a firearm or ammunition under 18 U.S.C 922(y)(2)—to legally purchase firearms, including high-capacity military-style rifles, with a valid hunting license or permit. A non-immigrant visa may be issued to a person with permanent residence outside the United States who wishes to be in the United States on a temporary basis. Examples of non-immigrant visas include student, tourist, and business visas. Although at least six states have enacted legislation to restrict non-citizens from purchasing or possessing firearms, [redacted] b7E

[redacted]

♦♦